

Practitioner's Docket No. 2189-19

PATENT

Preliminary Classification:

Proposed Class: 235

Subclass: 380

NOTE: "All applicants are requested to include a preliminary classification on newly filed patent applications. The preliminary classification, preferably class and subclass designations, should be identified in the upper right-hand corner of the letter of transmittal accompanying the application papers, for example 'Proposed Class 2, subclass 129.'" M.P.E.P. § 601, 7th ed.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Box Patent Application
Assistant Commissioner for Patents
Washington, D.C. 20231

NEW APPLICATION TRANSMITTAL

Transmitted herewith for filing is the patent application of

Inventor(s): Scott A. Vanstone

WARNING: 37 C.F.R. § 1.41(a)(1) points out:

"(a) A patent is applied for in the name or names of the actual inventor or inventors.

"(1) The inventorship of a nonprovisional application is that inventorship set forth in the oath or declaration as prescribed by § 1.63, except as provided for in § 1.53(d)(4) and § 1.63(d). If an oath or declaration as prescribed by § 1.63 is not filed during the pendency of a nonprovisional application, the inventorship is that inventorship set forth in the application papers filed pursuant to § 1.53(b), unless a petition under this paragraph accompanied by the fee set forth in § 1.17(i) is filed supplying or changing the name or names of the inventor or inventors."

For (title): TRANSACTION VERIFICATION PROTOCOL FOR SMART CARDS

CERTIFICATION UNDER 37 C.F.R. § 1.10*

(Express Mail label number is mandatory.)

(Express Mail certification is optional.)

I hereby certify that this New Application Transmittal and the documents referred to as attached therein are being deposited with the United States Postal Service on this date 26 July 1999, in an envelope as "Express Mail Post Office to Addressee," mailing Label Number EL440665367US, addressed to the: Assistant Commissioner for Patents, Washington, D.C. 20231.

EL440665367US

MARIAN CHRISTOPHER

(type or print name of person mailing paper)

Marian Christopher

Signature of person mailing paper

WARNING: Certificate of mailing (first class) or facsimile transmission procedures of 37 C.F.R. § 1.8 cannot be used to obtain a date of mailing or transmission for this correspondence.

WARNING: Each paper or fee filed by "Express Mail" must have the number of the "Express Mail" mailing label placed thereon prior to mailing. 37 C.F.R. § 1.10(b).

"Since the filing of correspondence under § 1.10 without the Express Mail mailing label thereon is an oversight that can be avoided by the exercise of reasonable care, requests for waiver of this requirement will not be granted on petition." Notice of Oct. 24, 1996, 60 Fed. Reg. 56,439, at 56,442.

(New Application Transmittal [4-1]—page 1 of 11)

1. Type of Application

This new application is for a(n)

(check one applicable item below)

- ☒ Original (nonprovisional)
☐ Design
☐ Plant

WARNING: Do not use this transmittal for a completion in the U.S. of an International Application under 35 U.S.C. § 371(c)(4), unless the International Application is being filed as a divisional, continuation or continuation-in-part application.

WARNING: Do not use this transmittal for the filing of a provisional application.

NOTE: If one of the following 3 items apply, then complete and attach **ADDED PAGES FOR NEW APPLICATION TRANSMITTAL WHERE BENEFIT OF A PRIOR U.S. APPLICATION CLAIMED** and a **NOTIFICATION IN PARENT APPLICATION OF THE FILING OF THIS CONTINUATION APPLICATION**.

- ☐ Divisional.
☒ Continuation.
☐ Continuation-in-part (C-I-P).

2. Benefit of Prior U.S. Application(s) (35 U.S.C. §§ 119(e), 120, or 121)

NOTE: A nonprovisional application may claim an invention disclosed in one or more prior filed copending nonprovisional applications or copending international applications designating the United States of America. In order for a nonprovisional application to claim the benefit of a prior filed copending nonprovisional application or copending international application designating the United States of America, each prior application must name as an inventor at least one inventor named in the later filed nonprovisional application and disclose the named inventor's invention claimed in at least one claim of the later filed nonprovisional application in the manner provided by the first paragraph of 35 U.S.C. § 112. Each prior application must also be:

(i) An international application entitled to a filing date in accordance with PCT Article 11 and designating the United States of America; or

(ii) Complete as set forth in § 1.51(b); or

(iii) Entitled to a filing date as set forth in § 1.53(b) or § 1.53(d) and include the basic filing fee set forth in § 1.16; or

(iv) Entitled to a filing date as set forth in § 1.53(b) and have paid therein the processing and retention fee set forth in § 1.21(f) within the time period set forth in § 1.53(f).

37 C.F.R. § 1.78(a)(1).

NOTE: If the new application being transmitted is a divisional, continuation or a continuation-in-part of a parent case, or where the parent case is an International Application which designated the U.S., or benefit of a prior provisional application is claimed, then check the following item and complete and attach **ADDED PAGES FOR NEW APPLICATION TRANSMITTAL WHERE BENEFIT OF PRIOR U.S. APPLICATION(S) CLAIMED**.

WARNING: If an application claims the benefit of the filing date of an earlier filed application under 35 U.S.C. §§ 120, 121 or 365(c), the 20-year term of that application will be based upon the filing date of the earliest U.S. application that the application makes reference to under 35 U.S.C. §§ 120, 121 or 365(c). (35 U.S.C. § 154(a)(2) does not take into account, for the determination of the patent term, any application on which priority is claimed under 35 U.S.C. §§ 119, 365(a) or 365(b).) For a c-i-p application, applicant should review whether any claim in the patent that will issue is supported by an earlier application and, if not, the applicant should consider canceling the reference to the earlier filed application. The term of a patent is not based on a claim-by-claim approach. See Notice of April 14, 1995, 60 Fed. Reg. 20,195, at 20,205.

(New Application Transmittal [4-1]—page 2 of 11)

WARNING: When the last day of pendency of a provisional application falls on a Saturday, Sunday, or Federal holiday within the District of Columbia, any nonprovisional application claiming benefit of the provisional application must be filed prior to the Saturday, Sunday, or Federal holiday within the District of Columbia. See 37 C.F.R. § 1.78(a)(3).

- ☐ The new application being transmitted claims the benefit of prior U.S. application(s). Enclosed are ADDED PAGES FOR NEW APPLICATION TRANSMITTAL WHERE BENEFIT OF PRIOR U.S. APPLICATION(S) CLAIMED.

3. Papers Enclosed

A. Required for filing date under 37 C.F.R. § 1.53(b) (Regular) or 37 C.F.R. § 1.153 (Design) Application

 7 Pages of specification

 4 Pages of claims

 2 Sheets of drawing

WARNING: DO NOT submit original drawings. A high quality copy of the drawings should be supplied when filing a patent application. The drawings that are submitted to the Office must be on strong, white, smooth, and non-shiny paper and meet the standards according to § 1.84. If corrections to the drawings are necessary, they should be made to the original drawing and a high-quality copy of the corrected original drawing then submitted to the Office. Only one copy is required or desired. For comments on proposed then-new 37 C.F.R. § 1.84, see Notice of March 9, 1988 (1990 O.G. 57-62).

NOTE: "Identifying indicia, if provided, should include the application number or the title of the invention, inventor's name, docket number (if any), and the name and telephone number of a person to call if the Office is unable to match the drawings to the proper application. This information should be placed on the back of each sheet of drawing a minimum distance of 1.5 cm. (5/8 inch) down from the top of the page . . ." 37 C.F.R. § 1.84(c)).

(complete the following, if applicable)

- ☐ The enclosed drawing(s) are photograph(s), and there is also attached a "PETITION TO ACCEPT PHOTOGRAPH(S) AS DRAWING(S)." 37 C.F.R. § 1.84(b).
- ☐ formal
- ☐ informal

B. Other Papers Enclosed

 1 Pages of declaration and power of attorney

 1 Pages of abstract

 Other

4. Additional papers enclosed

- ☐ Amendment to claims
- ☐ Cancel in this applications claims _____ before calculating the filing fee. (At least one original independent claim must be retained for filing purposes.)
- ☐ Add the claims shown on the attached amendment. (Claims added have been numbered consecutively following the highest numbered original claims.)
- ☐ Preliminary Amendment
- ☒ Information Disclosure Statement (37 C.F.R. § 1.98)
- ☒ Form PTO-1449 (PTO/SB/08A and 08B)
- ☐ Citations

- ☐ Declaration of Biological Deposit
- ☐ Submission of "Sequence Listing," computer readable copy and/or amendment pertaining thereto for biotechnology invention containing nucleotide and/or amino acid sequence.
- ☐ Authorization of Attorney(s) to Accept and Follow Instructions from Representative
- ☐ Special Comments
- ☐ Other

5. Declaration or oath (including power of attorney)

NOTE: A newly executed declaration is not required in a continuation or divisional application provided that the prior nonprovisional application contained a declaration as required, the application being filed is by all or fewer than all the inventors named in the prior application, there is no new matter in the application being filed, and a copy of the executed declaration filed in the prior application (showing the signature or an indication thereon that it was signed) is submitted. The copy must be accompanied by a statement requesting deletion of the names of person(s) who are not inventors of the application being filed. If the declaration in the prior application was filed under § 1.47, then a copy of that declaration must be filed accompanied by a copy of the decision granting § 1.47 status or, if a nonsigning person under § 1.47 has subsequently joined in a prior application, then a copy of the subsequently executed declaration must be filed. See 37 C.F.R. §§ 1.63(d)(1)-(3).

NOTE: A declaration filed to complete an application must be executed, identify the specification to which it is directed, identify each inventor by full name including family name and at least one given name, without abbreviation together with any other given name or initial, and the residence, post office address and country or citizenship of each inventor, and state whether the inventor is a sole or joint inventor. 37 C.F.R. § 1.63(a)(1)-(4).

- ☒ Enclosed Copy from parent application.

Executed by Scott A. Vanstone

(check all applicable boxes)

- ☒ inventor(s).
- ☐ legal representative of inventor(s).
37 C.F.R. §§ 1.42 or 1.43.
- ☐ joint inventor or person showing a proprietary interest on behalf of inventor who refused to sign or cannot be reached.
- ☐ This is the petition required by 37 C.F.R. § 1.47 and the statement required by 37 C.F.R. § 1.47 is also attached. See item 13 below for fee.

- ☐ Not Enclosed.

NOTE: Where the filing is a completion in the U.S. of an International Application or where the completion of the U.S. application contains subject matter in addition to the International Application, the application may be treated as a continuation or continuation-in-part, as the case may be, utilizing ADDED PAGE FOR NEW APPLICATION TRANSMITTAL WHERE BENEFIT OF PRIOR U.S. APPLICATION CLAIMED.

- ☐ Application is made by a person authorized under 37 C.F.R. § 1.41(c) on behalf of all the above named inventor(s).

(The declaration or oath, along with the surcharge required by 37 C.F.R. § 1.16(e) can be filed subsequently).

- ☐ Showing that the filing is authorized.
(not required unless called into question. 37 C.F.R. § 1.41(d))

6. Inventorship Statement

WARNING: If the named inventors are each not the inventors of all the claims an explanation, including the ownership of the various claims at the time the last claimed invention was made, should be submitted.

The inventorship for all the claims in this application are:

☒ The same.

or

☐ Not the same. An explanation, including the ownership of the various claims at the time the last claimed invention was made,

☐ is submitted.

☐ will be submitted.

7. Language

NOTE: An application including a signed oath or declaration may be filed in a language other than English. An English translation of the non-English language application and the processing fee of \$130.00 required by 37 C.F.R. § 1.17(k) is required to be filed with the application, or within such time as may be set by the Office. 37 C.F.R. § 1.52(d).

☒ English

☐ Non-English

☐ The attached translation includes a statement that the translation is accurate. 37 C.F.R. § 1.52(d).

8. Assignment

☒ An assignment of the invention to CERTICOM CORP., recorded
24 July 1997, Reel 8627, Frame 0863

☐ is attached. A separate ☐ "COVER SHEET FOR ASSIGNMENT (DOCUMENT) ACCOMPANYING NEW PATENT APPLICATION" or ☐ FORM PTO 1595 is also attached.

☐ will follow.

NOTE: "If an assignment is submitted with a new application, send two separate letters—one for the application and one for the assignment." Notice of May 4, 1990 (1114 O.G. 77-78).

WARNING: A newly executed "CERTIFICATE UNDER 37 C.F.R. § 3.73(b)" must be filed when a continuation-in-part application is filed by an assignee. Notice of April 30, 1993, 1150 O.G. 62-64.

(New Application Transmittal [4-1]—page 5 of 11)

9. Certified Copy

Certified copy(ies) of application(s)

Country	Appln. No.	Filed
Country	Appln. No.	Filed
Country	Appln. No.	Filed

from which priority is claimed

☐ is (are) attached.

☐ will follow.

NOTE: The foreign application forming the basis for the claim for priority must be referred to in the oath or declaration. 37 C.F.R. § 1.55(a) and 1.63.

NOTE: This item is for any foreign priority for which the application being filed directly relates. If any parent U.S. application or International Application from which this application claims benefit under 35 U.S.C. § 120 is itself entitled to priority from a prior foreign application, then complete item 18 on the ADDED PAGES FOR NEW APPLICATION TRANSMITTAL WHERE BENEFIT OF PRIOR U.S. APPLICATION(S) CLAIMED.

10. Fee Calculation (37 C.F.R. § 1.16)

A. ☒ Regular application

CLAIMS AS FILED			
Number filed	Number Extra	Rate	Basic Fee 37 C.F.R. § 1.16(a) \$760.00
Total Claims (37 C.F.R. § 1.16(c))	8 - 20 = 0	× \$ 18.00	0
Independent Claims (37 C.F.R. § 1.16(b))	2 - 3 = 0	× \$ 78.00	0
Multiple dependent claim(s), if any (37 C.F.R. § 1.16(d))		+ \$260.00	0

☐ Amendment cancelling extra claims is enclosed.

☐ Amendment deleting multiple-dependencies is enclosed.

☐ Fee for extra claims is not being paid at this time.

NOTE: If the fees for extra claims are not paid on filing they must be paid or the claims cancelled by amendment, prior to the expiration of the time period set for response by the Patent and Trademark Office in any notice of fee deficiency. 37 C.F.R. § 1.16(d).

Filing Fee Calculation

\$ 760

B. ☐ Design application
(\$310.00—37 C.F.R. § 1.16(f))

Filing Fee Calculation

\$

C. ☐ Plant application
(\$480.00—37 C.F.R. § 1.16(g))

Filing fee calculation

\$

11. Small Entity Statement(s)

- ☐ Statement(s) that this is a filing by a small entity under 37 C.F.R. § 1.9 and 1.27 is (are) attached.

WARNING: "Status as a small entity must be specifically established in each application or patent in which the status is available and desired. Status as a small entity in one application or patent does not affect any other application or patent, including applications or patents which are directly or indirectly dependent upon the application or patent in which the status has been established. The refiling of an application under § 1.53 as a continuation, division, or continuation-in-part (including a continued prosecution application under § 1.53(d)), or the filing of a reissue application requires a new determination as to continued entitlement to small entity status for the continuing or reissue application. A nonprovisional application claiming benefit under 35 U.S.C. § 119(e), 120, 121, or 365(c) of a prior application, or a reissue application may rely on a statement filed in the prior application or in the patent if the nonprovisional application or the reissue application includes a reference to the statement in the prior application or in the patent or includes a copy of the statement in the prior application or in the patent and status as a small entity is still proper and desired. The payment of the small entity basic statutory filing fee will be treated as such a reference for purposes of this section." 37 C.F.R. § 1.28(a)(2).

WARNING: "Small entity status must not be established when the person or persons signing the . . . statement can unequivocally make the required self-certification." M.P.E.P., § 509.03, 6th ed., rev. 2, July 1996 (emphasis added).

(complete the following, if applicable)

- ☐ Status as a small entity was claimed in prior application
_____ / _____, filed on _____, from which benefit
is being claimed for this application under:

35 U.S.C. § ☐ 119(e),
☐ 120,
☐ 121,
☐ 365(c),

and which status as a small entity is still proper and desired.

- ☐ A copy of the statement in the prior application is included.

Filing Fee Calculation (50% of A, B or C above)

\$ _____

NOTE: Any excess of the full fee paid will be refunded if small entity status is established and a refund request are filed within 2 months of the date of timely payment of a full fee. The two-month period is not extendable under § 1.136. 37 C.F.R. § 1.28(a).

12. Request for International-Type Search (37 C.F.R. § 1.104(d))

(complete, if applicable)

- ☐ Please prepare an international-type search report for this application at the time when national examination on the merits takes place.

13. Fee Payment Being Made at This Time

☒ Not Enclosed

☒ No filing fee is to be paid at this time.

(This and the surcharge required by 37 C.F.R. § 1.16(e) can be paid subsequently.)

☐ Enclosed

☐ Filing fee

\$ _____

☐ Recording assignment

(\$40.00; 37 C.F.R. § 1.21(h))

(See attached "COVER SHEET FOR
ASSIGNMENT ACCOMPANYING NEW
APPLICATION".)

\$ _____

☐ Petition fee for filing by other than all the
inventors or person on behalf of the inventor
where inventor refused to sign or cannot be
reached

(\$130.00; 37 C.F.R. §§ 1.47 and 1.17(i))

\$ _____

☐ For processing an application with a
specification in
a non-English language

(\$130.00; 37 C.F.R. §§ 1.52(d) and 1.17(k))

\$ _____

☐ Processing and retention fee

(\$130.00; 37 C.F.R. §§ 1.53(d) and 1.21(l))

\$ _____

☐ Fee for international-type search report

(\$40.00; 37 C.F.R. § 1.21(e))

\$ _____

NOTE: 37 C.F.R. § 1.21(f) establishes a fee for processing and retaining any application that is abandoned for failing to complete the application pursuant to 37 C.F.R. § 1.53(f) and this, as well as the changes to 37 C.F.R. §§ 1.53 and 1.78(a)(1), indicate that in order to obtain the benefit of a prior U.S. application, either the basic filing fee must be paid, or the processing and retention fee of § 1.21(f) must be paid, within 1 year from notification under § 53(f).

Total fees enclosed

\$ _____

14. Method of Payment of Fees

☐ Check in the amount of \$ _____

☐ Charge Account No. _____ in the amount of
\$ _____

A duplicate of this transmittal is attached.

NOTE: Fees should be itemized in such a manner that it is clear for which purpose the fees are paid. 37 C.F.R. § 1.22(b).

15. Authorization to Charge Additional Fees

WARNING: If no fees are to be paid on filing, the following items should not be completed.

WARNING: Accurately count claims, especially multiple dependent claims, to avoid unexpected high charges, if extra claim charges are authorized.

- ☐ The Commissioner is hereby authorized to charge the following additional fees by this paper and during the entire pendency of this application to Account No. _____.

☐ 37 C.F.R. § 1.16(a), (f) or (g) (filing fees)

☐ 37 C.F.R. § 1.16(b), (c) and (d) (presentation of extra claims)

NOTE: Because additional fees for excess or multiple dependent claims not paid on filing or on later presentation must only be paid or these claims cancelled by amendment prior to the expiration of the time period set for response by the PTO in any notice of fee deficiency (37 C.F.R. § 1.16(d)), it might be best not to authorize the PTO to charge additional claim fees, except possibly when dealing with amendments after final action.

☐ 37 C.F.R. § 1.16(e) (surcharge for filing the basic filing fee and/or declaration on a date later than the filing date of the application)

☐ 37 C.F.R. § 1.17(a)(1)–(5) (extension fees pursuant to § 1.136(a)).

☐ 37 C.F.R. § 1.17 (application processing fees)

NOTE: ". . . A written request may be submitted in an application that is an authorization to treat any concurrent or future reply, requiring a petition for an extension of time under this paragraph for its timely submission, as incorporating a petition for extension of time for the appropriate length of time. An authorization to charge all required fees, fees under § 1.17, or all required extension of time fees will be treated as a constructive petition for an extension of time in any concurrent or future reply requiring a petition for an extension of time under this paragraph for its timely submission. Submission of the fee set forth in § 1.17(a) will also be treated as a constructive petition for an extension of time in any concurrent reply requiring a petition for an extension of time under this paragraph for its timely submission." 37 C.F.R. § 1.136(a)(3).

☐ 37 C.F.R. § 1.18 (issue fee at or before mailing of Notice of Allowance, pursuant to 37 C.F.R. § 1.311(b))

NOTE: Where an authorization to charge the issue fee to a deposit account has been filed before the mailing of a Notice of Allowance, the issue fee will be automatically charged to the deposit account at the time of mailing the notice of allowance. 37 C.F.R. § 1.311(b).

NOTE: 37 C.F.R. § 1.28(b) requires "Notification of any change in status resulting in loss of entitlement to small entity status must be filed in the application . . . prior to paying, or at the time of paying, . . . the issue fee. . . ." From the wording of 37 C.F.R. § 1.28(b), (a) notification of change of status must be made even if the fee is paid as "other than a small entity" and (b) no notification is required if the change is to another small entity.

16. Instructions as to Overpayment

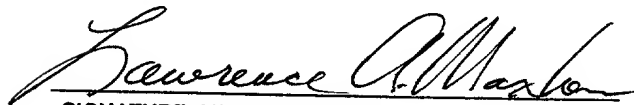
NOTE: "... Amounts of twenty-five dollars or less will not be returned unless specifically requested within a reasonable time, nor will the payer be notified of such amounts; amounts over twenty-five dollars may be returned by check or, if requested, by credit to a deposit account." 37 C.F.R. § 1.26(a).

- ☐ Credit Account No. _____
- ☐ Refund

Reg. No. 24,483

Tel. No. (619) 233-9004

Customer No.



SIGNATURE OF PRACTITIONER

LAWRENCE A. MAXHAM

(type or print name of attorney)

BAKER & MAXHAM

Symphony Towers

P.O. Address

750 "B" Street, Suite 3100
San Diego, California 92101

☒ **Incorporation by reference of added pages**

(check the following item if the application in this transmittal claims the benefit of prior U.S. application(s) (including an international application entering the U.S. stage as a continuation, divisional or C-I-P application) and complete and attach the ADDED PAGES FOR NEW APPLICATION TRANSMITTAL WHERE BENEFIT OF PRIOR U.S. APPLICATION(S) CLAIMED)

- ☒ Plus Added Pages for New Application Transmittal Where Benefit of Prior U.S. Application(s) Claimed

Number of pages added 5

- ☒ Plus Added Pages for Papers Referred to in Item 4 Above

Number of pages added 3

- ☐ Plus added pages deleting names of inventor(s) named in prior application(s) who is/are no longer inventor(s) of the subject matter claimed in this application.

Number of pages added _____

- ☐ Plus "Assignment Cover Letter Accompanying New Application"

Number of pages added _____

☐ **Statement Where No Further Pages Added**

(if no further pages form a part of this Transmittal, then end this Transmittal with this page and check the following item)

- ☐ This transmittal ends with this page.

ADDED PAGES FOR APPLICATION TRANSMITTAL WHERE BENEFIT OF
PRIOR U.S. APPLICATION(S) CLAIMED

NOTE: See 37 C.F.R. § 1.78.

17. Relate Back

WARNING: If an application claims the benefit of the filing date of an earlier filed application under 35 U.S.C. §§ 120, 121 or 365(c), the 20-year term of that application will be based upon the filing date of the earliest U.S. application that the application makes reference to under 35 U.S.C. §§ 120, 121 or 365(c). (35 U.S.C. § 154(a)(2) does not take into account, for the determination of the patent term, any application on which priority is claimed under 35 U.S.C. §§ 119, 365(a) or 365(b).) For a c-i-p application, applicant should review whether any claim in the patent that will issue is supported by an earlier application and, if not, the applicant should consider canceling the reference to the earlier filed application. The term of a patent is not based on a claim-by-claim approach. See Notice of April 14, 1995, 60 Fed. Reg. 20,195, at 20,205.

(complete the following, if applicable)

☒ Amend the specification by inserting, before the first line, the following sentence:**A. 35 U.S.C. § 119(e)**

NOTE: "Any nonprovisional application claiming the benefit of one or more prior filed copending provisional applications must contain or be amended to contain in the first sentence of the specification following the title a reference to each such prior provisional application, identifying it as a provisional application, and including the provisional application number (consisting of series code and serial number)." 37 C.F.R. § 1.78(a)(4).

☐ "This application claims the benefit of U.S. Provisional Application(s) No(s).:

APPLICATION NO(S).:

FILING DATE

____ / _____
____ / _____
____ / _____

____ "
____ "
____ "

B. 35 U.S.C. §§ 120, 121 and 365(c)

NOTE: "Except for a continued prosecution application filed under § 1.53(d), any nonprovisional application claiming the benefit of one or more prior filed copending nonprovisional applications or international applications designating the United States of America must contain or be amended to contain in the first sentence of the specification following the title a reference to each such prior application, identifying it by application number (consisting of the series code and serial number) or international application number and international filing date and indicating the relationship of the applications. . . . Cross-references to other related applications may be made when appropriate." (See § 1.14(a)). 37 C.F.R. § 1.78(a)(2).

- ☒ "This application is a
☒ continuation
☐ continuation-in-part
☐ divisional

of copending application(s)

- ☒ application number 08 / 90,545 filed on 1/30/97 "
☐ International Application filed on _____
_____ and which designated the U.S."

NOTE: The proper reference to a prior filed PCT application that entered the U.S. national phase is the U.S. serial number and the filing date of the PCT application that designated the U.S.

NOTE: (1) Where the application being transmitted adds subject matter to the International Application, then the filing can be as a continuation-in-part or (2) if it is desired to do so for other reasons then the filing can be as a continuation.

NOTE: The deadline for entering the national phase in the U.S. for an international application was clarified in the Notice of April 28, 1987 (1079 O.G. 32 to 46) as follows:

"The Patent and Trademark Office considers the International application to be pending until the 22nd month from the priority date if the United States has been designated and no Demand for International Preliminary Examination has been filed prior to the expiration of the 19th month from the priority date and until the 32nd month from the priority date if a Demand for International Preliminary Examination which elected the United States of America has been filed prior to the expiration of the 19th month from the priority date, provided that a copy of the international application has been communicated to the Patent and Trademark Office within the 20 or 30 month period respectively. If a copy of the international application has not been communicated to the Patent and Trademark Office within the 20 or 30 month period respectively, the international application becomes abandoned as to the United States 20 or 30 months from the priority date respectively. These periods have been placed in the rules as paragraph (h) of § 1.494 and paragraph (i) of § 1.495. A continuing application under 35 U.S.C. 365(c) and 120 may be filed anytime during the pendency of the international application."

- ☐ "The nonprovisional application designated above, namely application _____ / _____, filed _____, claims the benefit of U.S. Provisional Application(s) No(s).:

APPLICATION NO(S).:

FILING DATE

_____ / _____	_____ "
_____ / _____	_____ "
_____ / _____	_____ "

- ☐ Where more than one reference is made above, please combine all references into one sentence.

18. Relate Back—35 U.S.C. § 119 Priority Claim for Prior Application

The prior U.S. application(s), including any prior International Application designating the U.S., identified above in item 17B, in turn itself claim(s) foreign priority(ies) as follows:

Country	Appln. no.	Filed on
---------	------------	----------

The certified copy(ies) has (have)

- ☐ been filed on _____, in prior application 0 / _____, which was filed on _____
- ☐ is (are) attached.

WARNING: The certified copy of the priority application that may have been communicated to the PTO by the International Bureau may not be relied on without any need to file a certified copy of the priority application in the continuing application. This is so because the certified copy of the priority application communicated by the International Bureau is placed in a folder and is not assigned a U.S. serial number unless the national stage is entered. Such folders are disposed of if the national stage is not entered. Therefore, such certified copies may not be available if needed later in the prosecution of a continuing application. An alternative would be to physically remove the priority documents from the folders and transfer them to the continuing application. The resources required to request transfer, retrieve the folders, make suitable record notations, transfer the certified copies, enter and make a record of such copies in the Continuing Application are substantial. Accordingly, the priority documents in folders of international applications that have not entered the national stage may not be relied on. Notice of April 28, 1987 (1079 O.G. 32 to 46).

19. Maintenance of Copendency of Prior Application

NOTE: The PTO finds it useful if a copy of the petition filed in the prior application extending the term for response is filed with the papers constituting the filing of the continuation application. Notice of November 5, 1985 (1060 O.G. 27).

A. ☐ Extension of time in prior application:

(This item must be completed and the papers filed in the prior application, if the period set in the prior application has run.)

- ☐ A petition, fee and response extends the term in the pending prior application until _____

☐ A copy of the petition filed in prior application is attached.

B. ☐ Conditional Petition for Extension of Time in Prior Application

(complete this item, if previous item not applicable)

- ☐ A conditional petition for extension of time is being filed in the pending prior application.

☐ A copy of the conditional petition filed in the prior application is attached.

**20. Further Inventorship Statement Where Benefit of Prior Application(s)
Claimed**

(complete applicable item (a), (b) and/or (c) below)

- (a) ☒ This application discloses and claims only subject matter disclosed in the prior application whose particulars are set out above and the inventor(s) in this application are
- ☒ the same.
- ☐ less than those named in the prior application. It is requested that the following inventor(s) identified for the prior application be deleted:

(type name(s) of inventor(s) to be deleted)

- (b) ☐ This application discloses and claims additional disclosure by amendment and a new declaration or oath is being filed. With respect to the prior application, the inventor(s) in this application are
- ☐ the same.
- ☐ the following additional inventor(s) have been added:

(type name(s) of inventor(s) to be added)

- (c) The inventorship for all the claims in this application are
- ☒ the same.
- ☐ not the same. An explanation, including the ownership of the various claims at the time the last claimed invention was made
- ☐ is submitted.
- ☐ will be submitted.

21. Abandonment of Prior Application (if applicable)

- ☐ Please abandon the prior application at a time while the prior application is pending, or when the petition for extension of time or to revive in that application is granted, and when this application is granted a filing date, so as to make this application copending with said prior application.

NOTE: According to the Notice of May 13, 1983 (103, TMOG 6-7), the filing of a continuation or continuation-in-part application is a proper response with respect to a petition for extension of time or a petition to revive and should include the express abandonment of the prior application conditioned upon the granting of the petition and the granting of a filing date to the continuing application.

22. Petition for Suspension of Prosecution for the Time Necessary to File an Amendment

WARNING: *"The claims of a new application may be finally rejected in the first Office action in those situations where (A) the new application is a continuing application of, or a substitute for, an earlier application, and (B) all the claims of the new application (1) are drawn to the same invention claimed in the earlier application, and (2) would have been properly finally rejected on the grounds of art of record in the next Office action if they had been entered in the earlier application." M.P.E.P., § 706.07(b), 7th ed.*

NOTE: Where it is possible that the claims on file will give rise to a first action final for this continuation application and for some reason an amendment cannot be filed promptly (e.g., experimental data is being gathered) it may be desirable to file a petition for suspension of prosecution for the time necessary.

(check the next item, if applicable)

- ☐ There is provided herewith a Petition To Suspend Prosecution for the Time Necessary to File An Amendment (New Application Filed Concurrently)

23. Small Entity (37 C.F.R. § 1.28(a))

- ☐ Applicant has established small entity status by the filing of a statement in parent application /_____ on _____.
☐ A copy of the statement previously filed is included.

WARNING: See 37 C.F.R. § 1.28(a).

WARNING: *"Small entity status must not be established when the person or persons signing the . . . statement can unequivocally make the required self-certification." M.P.E.P., § 509.03, 7th ed. (emphasis added).*

24. NOTIFICATION IN PARENT APPLICATION OF THIS FILING

- ☒ A notification of the filing of this
(check one of the following)

- ☒ continuation
☐ continuation-in-part
☐ divisional

is being filed in the parent application, from which this application claims priority under 35 U.S.C. § 120.

TRANSACTION VERIFICATION PROTOCOL FOR SMART CARDS

The present invention relates to methods and apparatus for verifying the authenticity of partners in an electronic transaction.

5 It has become widely accepted to conduct transactions such that as financial transactions or exchange of documents electronically. In order to verify the transaction, it is also well-known to “sign” the transaction digitally so that the authenticity of the transaction can be verified. The signature is performed according to a protocol that utilizes the message, i.e. the transaction, and a secret key associated with the party. Any attempt to tamper with
10 the message or to use a key other than that of the signing party will result in an incompatibility between the message and the signature or will fail to identify the party correctly and thereby lead to rejection of the transaction.

The signature must be performed such that the parties’ secret key cannot be determined. To avoid the complexity of distributing secret keys, it is convenient to utilize a
15 public key encryption scheme in the generation of the signature. Such capabilities are available where the transaction is conducted between parties having access to relatively large computing resources but it is equally important to facilitate such transactions at an individual level where more limited computing resources are available.

Automated teller machines (ATMs) and credit cards are widely used for personal
20 transactions and as their use expands, so the need to verify such transactions increases. Transaction cards are now available with limited computing capacity, so-called “Smart Cards,” but these are not sufficient to implement existing digital signature protocols in a commercially viable manner. As noted above, in order to generate a digital signature, it is necessary to utilize a public key encryption scheme. Most public key schemes are based on
25 the Diffie Helman Public key protocol and a particularly popular implementation is that known as DSS. The DSS scheme utilizes the set of integers Z_p where p is a large prime. For adequate security, p must be in the order of 512 bits although the resultant signature may be reduced mod q , where q divides $p-1$, and may be in the order of 160 bits.

The DSS protocol provides a signature composed of two components r , s . The
30 protocol requires the selection of a secret random integer k from the set of integers $(0, 1, 2, \dots, q-1)$, i.e.

$$k \in \{0, 1, 2, \dots, q-1\}.$$

The component r is then computed such that

$$r = \{\beta^k \bmod p\} \bmod q$$

where β is a generator of q .

5 The component s is computed as

$$s = [k^{-1}(h(m)) + ar] \bmod q$$

where m is the message to be transmitted,

$h(m)$ is a hash of the message, and

a is the private key of the user.

10 The signature associated with the message is then s, r which may be used to verify the origin of the message from the public key of the user.

The value of β^k is computationally difficult for the DSS implementation as the exponentiation requires multiple multiplications mod p . This is beyond the capabilities of a “Smart Card” in a commercially acceptable time. Although the computation could be
15 completed on the associated ATM, this would require the disclosure of the session key k and therefore render the private key, a , vulnerable.

An alternative encryption scheme that provides enhanced security at relatively small modulus is that utilizing elliptic curves in the finite field 2^m . A value of m in the order of 155 provides security comparable to a 512 bit modulus for RSA and therefore offers significant
20 benefits in implementation. Diffie Helman Public Key encryption utilizes the properties of discrete logs so that even if a generator β and the exponentiation β^k is known, the value of k cannot be determined.

A similar property exists with elliptic curves where the addition of two points on a curve produces a third point on the curve. Similarly, multiplying a point by an integer k
25 produces a point on the curve.

However, knowing the point and the origin does not reveal the value of the integer ‘ n ’ which may then be used as a session key for encryption. The value kP , where P is an initial known point, is therefore equivalent to the exponentiation β^k .

Elliptic Curve Cryptosystems (ECC) offer advantages over other public key

cryptosystems when bandwidth efficiency, reduced computation, and minimized code space are application goals.

The preferred embodiment of the present invention discloses a protocol optimized for an ECC implementation for use with a "smartcard" having limited computing capacity. The protocol has been found to provide superior performance relative to other smartcard protocols and is achievable with an ECC implementation.

The protocol disclosed is appropriate for smartcard purchase applications such as those that might be completed between a terminal or ATM and a users personal card. The protocol provides a signature scheme which allows the card to authenticate the terminal without unnecessary signature verification which is an computationally intense operation for the smart card. The only signature verification required is that of the terminal identification (as signed by the certifying authority, or CA, which is essential to any such protocol. In the preferred embodiment, the protocol provides the card and terminal from fraudulent attacks from impostor devices, either a card or terminal.

In accordance with the invention there is provided A method of verifying a pair of participants in an electronic transaction to permit exchange of information therebetween, each of the participants includes a memory and having a respective private key t , a and public key Y_t , Y_c stored therein, the public keys derived from a generator α and a respective ones of the private keys t , a , the method comprising the steps of:

- (a) a first of the participants generating a unique transaction identification information PID upon initiation of the electronic transaction;
- (b) the first participant forwarding to a second participant the transaction identification information PID and a first certificate C1, the first certificate being signed by a certification authority according to a predetermined algorithm and including an identification information TIU ID unique to the first participant and the public information Y_t of the first participant;
- (c) the second participant verifying the first certificate C1, according to the predetermined algorithm, upon receipt thereof and extracting the identification information TIU ID and the public information Y_t therefrom;

- (d) the second participant, upon verification of the first certificate C1, generating a first random integer R2;
- (e) the second participant generating a first and second signature components r1, s1 utilizing the public key Y_1 of the first participant and the private key a of the second participant, respectively according to a predetermined protocol;
- (f) the second participant forwarding a message to the first participant, including the signature components r1, s1 and a second certificate C2 signed by the certification authority according to a predetermined algorithm and including an identification information CID unique to the second participant and the public information Y_c of the second participant;
- (g) the first participant verifying the second certificate C2 and extracting the identification information CID and public key Y_c and verifying the authenticity of the second participant by extracting the transaction identification information PID from the received message and comparing the received transaction identification information PID to the transmitted value;
- (h) the first participant extracting the first random integer R2 from the received message and transmitting the first random integer R2 to the second participant to acknowledge verification of the second participant; and
- (i) the second participant verifying the authenticity of the first participant by comparing the received first random integer R2 to the generated first random integer R2 and transmitting a second random integer R3 to the first participant to acknowledging verification of the first participant, thereby permitting exchange of information between the participants.

An embodiment of the invention will now be described by way of example only with reference to the accompanying drawings, in which:

Figure 1 is a diagrammatic representation of a scanning terminal and personal transaction card; and

Figure 2 is a chart that schematically illustrates the protocol.

Referring therefore to figure 1, a scanner terminal 10 has an inductive coupling 12 to cooperate with a card 14. When a card 14 is passed through the inductive coupling 12 a

transaction is recorded within a memory 16 on the card 14. Typically the transaction will debit the card with a set amount, e.g. an admission price, and the terminal 10 is credited a corresponding amount. The terminal is connected through a network to a central computer located at a financial institution that maintains records of transactions in a conventional manner.

To avoid fraudulent transactions being recorded at either the card or terminal the protocol shown in figure 2 is utilized.

Upon the scanner sensing the card through coupling 12, a unique purchase I.D. (PID) is generated by the terminal 10. The terminal 10 has a private key, t , stored in a secure location and a corresponding public key Y^t equal to α^t . The terminal 10 generates a message, M1, consisting of the purchase I.D. PID and the transaction amount, TA. It also appends to the message M1 a certificate signed by the certifying authority CA that includes terminal identification information TIU ID and the public key Y_t . The message M1 is received by the card 14.

Card 14 has a private key a stored securely in memory 16 and a public key Y_a equal to α^a . (α is the generator point for the curve). The card verifies the terminal's certificate as signed by the certifying authority CA according to a normal elliptic curve scheme. Having verified the certificate, the card generates a pair of random numbers R2 and R3 and signs the unique purchase I.D. PID using the terminal's public key according to an established protocol.

To effect signing, the card generates a random integer k and computes a session parameter α^k . It also computes Y_t^k and generates signature components $r1$ and $s1$.

The component $r1$ is provided by $M2 \cdot Y_t^k \bmod L$ where:

M2 is the message TA//TIU ID//R2//PID, and

$L = 2^l - 1$ and l is an integer greater or equal to the number of bits in M2. (l signifies concentration).

The component $s1$ is provided by $h \cdot a + k \bmod q$ where:

q is the order of the curve and

h is a hash $h(M2//\alpha^k//R3)$.

The card now sends signature components $r1$, $s1$ the hash h and a certificate issued by

the certifying authority CA containing its ID and public key to the terminal 10.

The terminal verifies the cards credentials as signed by the CA. Given the hash h and s_1 it can calculate the value α^{kt} and thereby recover the message M_2 from r_1 using the cards public key. As the message M_2 includes the PID, the terminal is able to verify the authenticity if the card 10.

The recovered message includes R_2 which is then returned to the card 10 to prove that the terminal is extracting R_2 in real time, i.e. during the transit of the card through the coupling 12, using its private key. This also prevents a reply attack by the terminal 10.

The receipt of R_2 also serves to acknowledge provision of the service. Upon receipt, the card checks R_2 to ensure the message was recovered using the terminals private key. This confirms that the card was talking to the terminal rather than a fraudulent device which would not have the private key, t , available.

If the card confirms the receipt of R_2 , it transmits the random R_3 to the terminal 10 to complete the transaction. R_3 is required for card signature verification by the bank and so R_3 is retained by the terminal 10 for central processing purposes. R_3 is not released by the card until it has received R_2 which confirms that the terminal 10 is performing computations in real time.

The terminal 10 is required to submit to the financial institution the stored values of R_2 , R_3 , TA , PID , TIU ID, s_1 and α^k in addition to the credentials of both card and terminal 10. With this information the bank card is able to reproduce hash h , i.e. $h(M_2//\alpha^k//R_3)$ by using the cards public key Y_c to prove that the transaction was authentic.

It will be noted that the last two passes are essentially trivial and do not require computation. Accordingly the computation required by the card is minimal, being restricted to one verification and one signature that involves two exponentiations, with the balance avoiding computationally intense operations.

As indicated in figure 2, an ECC implementation is the field 2^{155} using an anomalous curve of this protocol would result in less bandwidth (1533 bits) and reduced computation for the smartcard (31,000 clock cycles). The computational savings over previous protocols are possible due to features of the elliptic curve signature scheme used by the smartcard.

The particular benefits and attributes may be summarized as:

1. The purchase identifier PID is unique and is required to prevent terminal replay to the bank. If the purchase identifier is not unique, a random number R1 will also be required to provide the equivalent of the PID.
2. The random bit string R2 is required to prevent replay to the card.
3. A hash function (h) such as the SHA1 is required to prevent modification of the message (m) and the terminal's identification (TIU ID).
4. There appears to be no advantage to having the transaction amount signed by the terminal, resulting in one less signature verification for the card. The reason for this is that the message signed by the card contains a random number R2 which can only be recovered by the terminal.
5. Using this scheme, the message m may only be recovered by the terminal (note the terminal's public key is used in step III therefore requiring the terminal's private key to verify and recover contents). By demonstrating to the card that the random string (R2) was obtained from the message, the terminal can be authenticated to the card.

We Claim:

1. A method of verifying a pair of participants in an electronic transaction to permit exchange of information therebetween, each of said participants includes a memory and having a
5 respective private key t , a and public key Y_t , Y_a stored therein, said public keys derived from a generator α and a respective ones of said private keys t , a , said method comprising the steps of:

(a) a first of said participants generating a unique transaction identification information PID upon initiation of said electronic transaction;

10 (b) said first participant forwarding to a second participant said transaction identification information PID and a first certificate C1, said first certificate being signed by a certification authority according to a predetermined algorithm and including an identification information TIU ID unique to said first participant and said public information Y_t of said first participant;

15 (c) said second participant verifying said first certificate C1, according to said predetermined algorithm, upon receipt thereof and extracting said identification information TIU ID and said public information Y_t therefrom;

(d) said second participant, upon verification of said first certificate C1, generating first and second random integers R2 and R3, respectively;

20 (e) said second participant generating a third random integer k and computing a session parameter α^k by exponentiating a function including said generator to a power k and exponentiating said public key Y_t to a power k to produce a session key Y_t^k ;

(f) said second participant generating a first signature component $r1$ by signing said transaction identification information PID utilizing said public key Y_t of said first
25 participant and generating a second signature component $s1$ by signing said first random integer R2 utilizing said private key a of said second participant, said signatures being generated according to a predetermined protocol;

(g) said second participant forwarding a message to said first participant, including said signature components $r1$, $s1$ and a second certificate C2 signed by said certification

authority according to a predetermined algorithm and including an identification information CID unique to said second participant and said public information Y_c of said second participant;

5 (h) said first participant verifying said second certificate C2 and extracting said identification information CID and public key Y_c and verifying the authenticity of said second participant by extracting said transaction identification information PID from said received message and comparing said received transaction identification information PID to said transmitted value;

10 (i) said first participant extracting said first random integer R2 from said received message and transmitting said first random integer R2 to said second participant to acknowledge verification of said second participant;

15 (j) said second participant verifying the authenticity of said first participant by comparing said received first random integer R2 to said generated first random integer R2 and transmitting said second random integer R3 to said first participant to acknowledging verification of said first participant, thereby permitting exchange of information between said participants.

20 3. A method as defined in claim 1, wherein said first participant forwards a transaction amount TA with said identification PID.

25 4. A method as defined in claim 1, wherein said first signature component $r1$ combines said session key Y_t^k and a message M2, indicative of the concatenation of said identification information TIU ID, said first random information R2, and said transaction identification information PID.

5. A method as defined in claim 3, wherein said first signature component $r1$ is of the form $M2 * Y_t^k \bmod L$.

6. A method as defined in claim 3, wherein said second signature component $s1$ is of the form $h*a + k \bmod q$, where q is the order of an elliptic curve, h is a hash of the concatenation of said second random integer $R3$, said session parameter α^k and said message $M2$.

5

7. A method as defined in claim 5, including in step (g) of claim 1 forwarding said hash to said first participant.

8. A method of verifying a pair of participants in an electronic transaction to permit exchange of information therebetween, each of said participants includes a memory and having a respective private key t , a and public key Y_t , Y_c stored therein, said public keys derived from a generator α and a respective ones of said private keys t , a , said method comprising the steps of:

10

(a) a first of said participants generating a unique transaction identification information PID upon initiation of said electronic transaction;

15

(b) said first participant forwarding to a second participant said transaction identification information PID and a first certificate $C1$, said first certificate being signed by a certification authority according to a predetermined algorithm and including an identification information $TIU\ ID$ unique to said first participant and said public information Y_t of said first participant;

20

(c) said second participant verifying said first certificate $C1$, according to said predetermined algorithm, upon receipt thereof and extracting said identification information $TIU\ ID$ and said public information Y_t therefrom;

(d) said second participant, upon verification of said first certificate $C1$, generating a first random integer $R2$;

25

(e) said second participant generating a first and second signature components $r1$, $s1$ utilizing said public key Y_t of said first participant and said private key a of said second participant, respectively according to a predetermined protocol;

- (f) said second participant forwarding a message to said first participant, including said signature components r_1 , s_1 and a second certificate C_2 signed by said certification authority according to a predetermined algorithm and including an identification information CID unique to said second participant and said public information Y_c of said second participant;
- (g) said first participant verifying said second certificate C_2 and extracting said identification information CID and public key Y_c and verifying the authenticity of said second participant by extracting said transaction identification information PID from said received message and comparing said received transaction identification information PID to said transmitted value;
- (h) said first participant extracting said first random integer R_2 from said received message and transmitting said first random integer R_2 to said second participant to acknowledge verification of said second participant; and
- (i) said second participant verifying the authenticity of said first participant by comparing said received first random integer R_2 to said generated first random integer R_2 and transmitting a second random integer R_3 to said first participant to acknowledging verification of said first participant, thereby permitting exchange of information between said participants.

ABSTRACT

A protocol appropriate for smartcard purchase applications such as those that might be completed between a terminal or ATM and a users personal card is disclosed. The protocol provides a signature scheme which allows the card to authenticate the terminal without unnecessary signature verification which is an computationally intense operation for the smart card. The only signature verification required is that of the terminal identification (as signed by the certifying authority, or CA, which is essential to any such protocol). In the preferred embodiment, the protocol provides the card and terminal from fraudulent attacks from impostor devices, either a card or terminal.

10

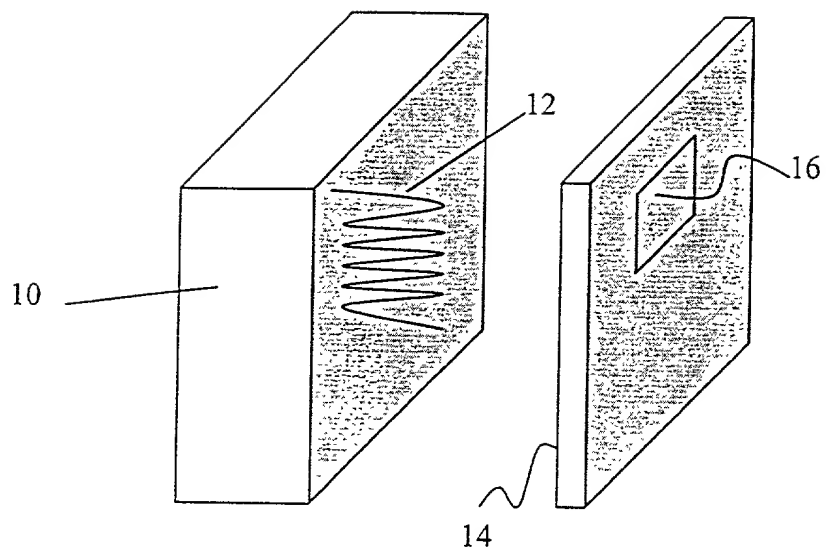


Figure 1


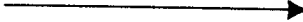
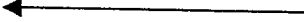
Smartcard Action	Transmission	Terminal Action
		Generate unique purchase ID and create transaction message
	 Purchase ID, TA 220 bits [TIU ID, Y_T] CA 355 bits	
Verify Certificate signed by CA 15,500 clock cycles Generate Random Number (R2) and sign transaction number using terminal's public key 15,500 clock cycles		
Send signed transaction data, hash and certificate signed by CA	 [r1,s1] card 375 bits Hash 128 bits [Smartcard ID, Smartcard Public Key] CA 355 bits	
		Verify Certificate signed by CA Given the hash h and s1, deduce α^{k^T} session key Recover message from r1
	R2 100 bits	Send R2 contained in message to card to prove identity and to acknowledge the provision of service
Check R2 to complete transaction		
Total computation time = 31,000 clock cycles	Total bits transmitted = 1533	

Figure 2

INVENTOR'S OATH AND AFFIDAVIT FOR PATENT APPLICATION

Docket Number: 2189-13 LAM

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name. I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

TRANSACTION VERIFICATION PROTOCOL FOR SMART CARDS, the specification of which is attached hereto unless the following is checked:

☒ was filed on 30 January 1997 as United States Application Number _____

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to patentability as defined in Title 37, Code of Federal Regulations, § 1.56. I hereby claim foreign priority benefits under Title 35, United States Code, § 119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed.

Prior Foreign Application(s)

<u>9601924.5</u>	<u>U.K.</u>	<u>31 January 1996</u>	Priority Claimed
(Number)	(Country)	(Day/Month/Year Filed)	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
_____	_____	_____	<input type="checkbox"/> Yes <input type="checkbox"/> No
(Number)	(Country)	(Day/Month/Year Filed)	

I hereby claim the benefit under Title 35, United States Code, § 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, § 112, I acknowledge the duty to disclose information which is material to patentability as defined in Title 37, Code of Federal Regulations, § 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application.

_____	_____	_____
(Application Number)	(Filing Date)	(Status - patented, pending, abandoned)
_____	_____	_____
(Application Number)	(Filing Date)	(Status - patented, pending, abandoned)

I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and to transact all business in the U.S. Patent and Trademark Office connected therewith: Frederic E. Baker, Reg. #24,078; Lawrence A. Maxham, Reg. #24,483; Michael H. Jester, Reg. #28,022; Terrance A. Meador, Reg. #30,298; David A. Hall, Reg. #32,233; Dan L. Hubert, Reg. #32,233; Bruce W. Greenhaus, Reg. #37,338; and Ervin F. Johnston, Reg. #20,190. Address of telephone calls to Lawrence A. Maxham at Telephone No. (619) 233-9004 and address all correspondence to Lawrence A. Maxham, BAKER, MAXHAM, JESTER & MEADOR, 750 "B" Street, Suite 3100, San Diego, California 92101.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true, and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full name of sole or first inventor, (given name, family name) SCOTT A. YANSTONE

Inventor's signature [Signature] Date May 30, 1997
 Residence Windsor, Ontario, Canada Citizenship Canada
 Post Office Address 589 Sandbrook Court, Windsor, Ontario N2T 2R4, Canada

Full name of second joint inventor, if any (given name, family name) _____

Inventor's signature _____ Date _____
 Residence _____ Citizenship _____
 Post Office Address _____

____ Additional inventors are being named on separately numbered sheets attached hereto.

(292 PTO)